University of California

UC HIPAA Glossary

The University's Health Information Privacy Policies are intended to implement applicable provisions of Health Insurance Portability & Accountability Act (HIPAA) Administrative Simplification regulations. The HIPAA regulations are complex and include a large number of defined terms. This glossary consists of all technical terms on which the University's health information policies are based that have been derived from the HIPAA regulations or California law, either as a verbatim restatement of the source term or a reasonable simplification of the term to better correspond to University operations. Also included are several terms specific to University operations that are not defined in the HIPAA regulations or California law, and a listing of commonly used acronyms.

In each separate policy, the definitions to be included in the policy may be limited to terms specific to that policy. Therefore, the reader should use this UC HIPAA Glossary for definitions of terms that may not appear in the specific policy. In general, defined terms in the University Health Information Privacy policies are indicated by initial character capitalization.

All section references in the definitions are references to Title 45 of the Code of Federal Regulations (CFR) Parts 160, 162 and 164, the HIPAA Administrative Simplification Regulation Text, U.S. Department of Health and Human Services, and the Office for Civil Rights, unless otherwise specified. The section references are included for information only and are not part of the definition.

A list of commonly used Acronyms is provided at the end of the “Definitions” section.

Definitions

Access means, in connection with HIPAA security standards for the protection of electronic Protected Health Information, the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. [45 CFR 164.304.]

Addressable means, with reference to a Security Rule standard or a specific implementation specification of the standard, that the Health Care Component must assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity’s electronic Protected Health Information; and (a) must implement the specification if reasonable and appropriate; or (b) if implementing the specification is not reasonable and appropriate, must document why it would not be reasonable and appropriate to implement the specification; and (c) must implement an equivalent alternative measure if reasonable and appropriate. [45 CFR 164.306 (d).]

Administrative Safeguards are administrative actions, policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect

electronic Protected Health Information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. [45 CFR 164.304.]

Affiliated Covered Entities (ACEs) are legally separate covered entities that are under common ownership or control and that have collectively designated themselves as a single affiliated covered entity for the purposes of the Privacy and Security Rule and have documented the designation. [45 CFR 164.105(b).]

American Recovery and Reinvestment Act of 2009 (ARRA) or the federal "economic stimulus" bill signed into law on February 17, 2009. The ARRA provides the statutory authority for HHS' breach notification regulations.

Authentication means the corroboration that a person is the one claimed. [45 CFR 164.304.]

Authorization means the granting of permission to share specific information with a specific party for a specific purpose. [45 CFR 164.508.]

Availability means the property that data or information is accessible and useable upon demand by an authorized person. [45 CFR 164.304.]

Breach means the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. Breach does not include the following circumstances:

> (1) any unintentional acquisition, access, or use of Protected Health Information by an employee or individual acting under the authority of a covered entity or business associate if (i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and (ii) such information is not further acquired, accessed, used, or disclosed by any person;
>
> (2) any inadvertent disclosure from an individual who is otherwise authorized to access Protected Health Information at a facility operated by a covered entity or business associate to another similarly situated individual at the same facility; and any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person; or
>
> (3) a situation in which an unauthorized person to whom the information is disclosed would not reasonably be able to retain the information (e.g., PHI that was sent out by the post office is returned unopened, as undeliverable).
>
> [HITECH Act § 13400 (42 U.S.C. § 17921); see also 74 Fed. Reg. 42,740 (Aug. 24, 2009).]

Breach of the Security of the System (Security System Breach) [California law] means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure. [California Civil Code §1798.29,

applicable to any agency that owns or licenses computerized data that includes personal information; restated in California Civil Code §1798.82, applicable to any person or business, including a Business Associate, that conducts business in California, and that owns or licenses computerized data that includes personal information. "Personal Information" means an individual's first name or first initial and last name in combination with any of a number of data elements (e.g., social security number, driver's license number, medical information, account number, etc.).]

Business Associate (BA) means a person, contractor, vendor, institution, or other entity that, on behalf of the SHCC or SHPC, but other than in the capacity of a member of the SHCC or SHPC workforce, performs, or assists in the performance of:

- A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing; or
- Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for the Health Care Component, or to or for an organized health care arrangement in which the Health Care Component participates, where the provision of the service involves the disclosure of individually identifiable health information from the Health Care Component or arrangement, or from another business associate of the Health Care Component or arrangement, to the person.

The University's SHCC or SHPC may be a business associate of another covered entity. [45 CFR 160.103.] If an Organized Health Care Arrangement (as defined herein) performs a "business associate" function (see bullet points above) for or on behalf of such Organized Health Care Arrangement, it does not, through the mere performance of these activities, become a Business Associate of other entities participating in such Organized Health Care Arrangement.

Business Associate Agreement (BAA) means a contract or an agreement entered into by the University on behalf of the University's SHCC or SHPC or a component of the University's SHCC or SHPC with an outside entity functioning as a business associate of the University; or an agreement entered into by the University as a business associate of another covered entity. A BAA must comply with the specifications for such agreements set out in the HIPAA regulations. [45 CFR 164.314.]

The ***Common Rule*** governs research involving living individuals that is conducted or supported by 15 named federal departments and agencies. The regulation also applies to research that is not federally supported but that institutions have voluntarily agreed will comply with federal standards. The Common Rule generally requires that:

- Federally supported research be reviewed by an ethics committee, sometimes referred to as an Institutional Review Board (IRB), that is comprised of at least five individuals, one of whom must be unaffiliated with the research institution. The Common Rule establishes standards for IRB approval of research, including provisions permitting approval of a proposal only if risks to subjects have been

minimized and are reasonable in relation to anticipated benefits and the importance of knowledge that may reasonably be expected to result;

- Individuals who participate in covered research are selected equitably and are permitted to participate only after giving informed, voluntary consent, unless the IRB has approved a waiver of consent; and
- Grantee institutions execute an assurance of compliance with the Common Rule (referred to as a "Federal-wide Assurance" or "FWA").

[45 CFR 46, Subpart A.]

Confidentiality of Medical Information Act (CMIA) means Part 2.6 of Division 1, commencing with Section 56 of the California Civil Code, which regulates the uses and disclosures of individually identifiable medical information by licensed health care professionals and other health care provider entities in California. [California Civil Code Section 56, *et seq*.]

Confidentiality means the property that data or information is not made available or disclosed to unauthorized persons or processes. [45 CFR 164.304.]

Contrary, when used to compare a provision of California state law to a HIPAA regulatory standard, requirement, or implementation specification, means that (1) a covered entity would find it impossible to comply with both the California and federal requirements; or (2) the provision of California law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of HIPAA. [45 CFR 160.202.]

Covered Entity (CE) means a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with furnishing, billing, or receiving payment for health care. [45 CFR 160.103.]

Covered Functions means those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse. [45 CFR 164.103.]

Covered Health Care Provider means a health care provider who transmits any health information in electronic form in connection with furnishing, billing, or receiving payment for health care in the normal course of business. [45 CFR 162.402 and 160.103.]

Data Aggregation means, with respect to Protected Health Information created or received by a business associate, the combining of such Protected Health Information with other Protected Health Information received by the business associate from another covered entity, to allow the business associate to create data analyses that relate to the health care operations of the respective covered entities. [45 CFR 164.501.]

Data Use Agreement (DUA) means a required document under HIPAA that provides satisfactory assurances to the SHCC that the recipient of a Limited Data Set provided to the recipient by the SHCC will only use or disclose the Protected Health Information contained in the Limited Data Set for specified purposes. The Data Use Agreement has specific content requirements. [45 CFR 164.514(e)(4).]

De-Identified Data means data or a health information data set that does not contain any of the Identifiers that could serve to identify the individual or individuals associated with the health information. [45 CFR 164.514.]

De-Identified Health Information means health information that does not identify an individual and where there is no reasonable basis to believe that the information can be used to identify the individual. De-identified health information does not constitute individually identifiable health information. Removal of all Identifiers of a medical or other health record results in De-Identified Health Information. [45 CFR 164.514.]

Department of Health & Human Services (DHHS) is the federal agency which, together with its Office of Civil Rights (OCR), is responsible for developing, promulgating and enforcing HIPAA rules, standards and implementation guidelines.

Designated Record Set (DRS) means a group of records maintained by or for a covered entity that:

- Includes the medical records and billing records about individuals maintained by or for a covered health care provider;
- Includes the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Is used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term “record” means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a covered entity. [45 CFR 164.501.]

Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information. [45 CFR 160.103.]

Electronic Media means:

- Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or
- Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/ transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

[45 CFR 160.103.]

Electronic Protected Health Information (EPHI) means Protected Health Information that is transmitted by electronic media or is maintained in electronic media. [45 CFR 160.103.]

Employer means the person for whom an individual performs or performed any service, of whatever nature, as the employee of such person, except that if the person for whom the individual performs or performed the services does not have control of the payment of the wages for such services, the term “employer” means the person having control of the payment of such wages. [45 CFR 160.103]

Encryption means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key and that process or key that would allow decryption has not been reached. HHS has identified certain encryption processes that meet this standard, including encryption processes for (i) data at rest that are consistent with NIST Special Publication 800-111 (Guide to Storage Encryption Technologies for End User Devices) and (ii) data in motion that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2. [45 CFR 164.304.]

Facility means the physical premises and the interior and exterior of a building(s). [45 CFR 164.304.]

Group Health Plan means an employee welfare benefit plan, including insured and self-insured plans, to the extent that the plan provides medical care, including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that: (1) has 50 or more participants; or (2) is administered by an entity other than the employer that established and maintains the plan. [45 CFR 160.103.]

Health Care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following:

- Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual, or that affects the structure or function of the body; and
- The sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. [45 CFR 160.103.]

Health Care Component means a component or combination of components of the University’s SHCC as designated and documented by the SHCC. [45 CFR 164.103.]

Health Care Operations means any of the following activities of any of the Health Care Components of the SHCC to the extent that the activities are related to covered functions:

- Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training

programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

- Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
- Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- Business management and general administrative activities of the covered entity, including, but not limited to:

    A. Management activities relating to implementation of and compliance with the HIPAA requirements;

    B. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that Protected Health Information is not disclosed to such policy holder, plan sponsor, or customer;[cf. Organized Health Care Arrangement]

    C. Resolution of internal grievances;

    D. The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity;

    E. The creation of de-identified health information or a limited data set, and

    F. Fundraising for the benefit of a health care component of the SHCC.

[45 CFR 164.501.]

Health Care Provider means any person or organization who provides medical or health services, including a hospital, a critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. [45 CFR 160.103.]

Health Information means any information, whether oral or recorded in any form or medium, that:

- Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

- Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. [45 CFR 160.103.]

Health Information Technology for Economic and Clinical Health (HITECH) Act appears as Title XIII of Division A of ARRA and contains financial incentives to assist hospitals in adopting electronic health record (EHR) systems and enhancements to HIPAA privacy and security regulations, including new HIPAA privacy breach notification requirements that went into effect September 17, 2009.

Health Insurance Information [California] means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. [California Civil Code §1798.82]

Health Insurance Portability & Accountability Act (HIPAA) is the federal law adopted in 1996 that resulted in the codification of regulations by DHHS in Title 45 Code of Federal Regulations Parts 160, 162, and 164 that contain Administrative Simplification provisions to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers and that establish standards for the security and privacy of health data. Congress intended these standards to create efficiencies in the health care system by encouraging the use of electronic data.

Health Oversight Agency means an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. [45 CFR 164.501.]

Health Plan means individual or group plans(including HMOs, health insurance issuers, and employee welfare benefit plans), either privately insured or self-insured, that are programs of the University of California that provide medical care, or pay the cost of medical care. A plan or program provides for medical care if it provides treatment or payment activities to an individual. University health plans include various medical, dental and vision plans, health care flexible spending accounts, and employee assistance programs offered to employees and their dependents. [45 CFR 160.103.]

Hybrid Entity means a single legal entity that is a covered entity, whose business activities include both covered and non-covered functions; and that designates health care components. The University is a Hybrid Entity. [45 CFR 164.103.]

Identifier means any of the following elements that can be used to identify individuals or their relatives, household members, or employers:

- Names;
- All geographic subdivisions smaller than a state, including street address, city, county,

precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;

- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except as permitted for dates, as described above.

[45 CFR 164.514 (b)(2).]

Implementation Specifications are specific requirements or instructions for implementing a HIPAA standard. [45 CFR 160.103.]

Individual means the person who is the subject of Protected Health Information. [45 CFR 160.103.]

Individually identifiable [California] means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social

security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. [CMIA, California Civil Code 56.05 (g).]

Individually Identifiable Health Information (IIHI) means health information, including demographic information collected from an individual, that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. [45 CFR 160.103.]

Information System (IS) means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. [45 CFR 164.304.]

Institutional Review Board (IRB) means the board or committee established at a University location that is responsible for the review and protection of all human subject research to be conducted at or under the direction of researchers at the location.

Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner. [45 CFR 164.304.]

Licensed Facility [California] means a clinic, health facility, home health agency, or hospice licensed pursuant to §§ 1204, 1250, 1725, or 1745 of the California Health & Safety Code. For the purposes of this policy, the unauthorized access notification requirements of Health & Safety Code § 1280.15 only apply to Licensed Facilities. [California Health & Safety Code § 1280.15, as amended by Senate Bill No. 541, effective January 1, 2009.]

Licensed Health Care Professional [California] means any person licensed or certified by the State of California pursuant to Division 2 (commencing with Section 500) of the Business and Professions Code, the Osteopathic Initiative Act or the Chiropractic Initiative Act, or Division 2.5 (commencing with Section 1797) of the Health and Safety Code. [California Civil Code 56.05(e).]

Limited Data Set (LDS) is Protected Health Information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;

- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images. [45 CFR 164.514.]

Malicious Software means software (for example, a computer virus) designed to damage or disrupt a system. [45 CFR 164.304.]

Marketing is defined in two ways:

(1) A communication about a product or service that encourages recipients of the communication to purchase or use the product or service; or

(2) An arrangement between the SHCC and any other entity whereby (a) the SHCC sells or otherwise receives indirect or direct remuneration for disclosing PHI to the other entity; and (b) the other entity or its affiliate uses the PHI to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

A communication that falls within definition (1) is *excluded* from the definition of "marketing" (i.e., prior Authorization is not required) as long as it meets the following criteria:

- The SHCC <u>does not receive direct or indirect payment</u> for the communication; **and**
- The communication describes a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; **or**
- The communication is for treatment of the individual; **or**
- For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual.

<u>However, even if the SHCC received direct or indirect payment for the above communications, the communications are nonetheless excluded from the definition of marketing if one of the following three scenarios apply</u>:

- **Scenario (1):**

  (i) the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication; and

  (ii) any payment received by such covered component in exchange for making a communication described in clause (i) is reasonable in amount; **or**

- **Scenario (2):**

  (i) the communication is made by the covered component; and

  (ii) the covered component making such communication obtains from the recipient of the communication a valid HIPAA Authorization with respect to such communication; **or**

- **Scenario (3):**

  (i) the communication is made by a business associate on behalf of the covered component; and

  (ii) the communication is consistent with the business associate agreement between such business associate and covered component; and

  (iii) the communication does not involve the use of PHI to promote an activity or product of the business associate or another third party.

[45 CFR 164.501; HITECH § 13406.]

Medical Information, for purposes of compliance with **California Civil Code § 1798.82**, means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. [California Civil Code §1798.82]

Medical Information, for purposes of compliance with **CMIA,** means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment. "Individually identifiable" means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity. [CMIA, California Civil Code 56.05 (g).]

More Stringent, in the context of a comparison of a provision of state law and a HIPAA Privacy Rule requirement or standard (*excluding* the breach notification rule found at Subpart D of Title 45, Part 164), means a state law that meets one or more of the following criteria:

- the law prohibits or restricts a use or disclosure of Individually Identifiable Health Information in circumstances under which such use or disclosure otherwise would be permitted under the HIPAA Privacy Rule, except if the disclosure is required in connection with a HIPAA compliance inquiry by DHHS or the disclosure is to the individual who is the subject of the health information;

- the law permits greater rights of access or amendment, as applicable, to the individual who is the subject of the health information;
- the law provides the greater amount of information about a use, a disclosure, rights, and remedies to the individual who is the subject of the health information;
- the law provides requirements that narrow the scope or duration, increase the privacy protections afforded, or reduce the coercive effect of the circumstances surrounding the express legal permission, as applicable, from the individual who is the subject of the health information;
- the law provides for the retention or reporting of more detailed accounting of disclosure information to the individual, or for a longer duration;
- with respect to any other matter, the law provides greater privacy protection for the individual who is the subject of the health information. [45 CFR 160.202.]

Organized Health Care Arrangement (OHCA) means:

- A clinically-integrated care setting in which individuals typically receive health care from more than one health care provider;
- An organized system of health care in which more than one Covered Entity participates and in which the participating Covered Entities:

  A. Hold themselves out to the public as participating in a joint arrangement; and

  B. Participate in joint activities that include at least one of the following:

     i. Utilization review, in which health care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf;

     ii. Quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or

     iii. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
- A Group Health Plan and a health insurance issuer or HMO with respect to such Group Health Plan, but only with respect to Protected Health Information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such Group Health Plan;
- A Group Health Plan and one or more other Group Health Plans each of which are maintained by the same plan sponsor; or

- The Group Health Plans described in the bullet above (i.e., a Group Health Plan and one or more other Group Health Plans that are maintained by the same plan sponsor) and health insurance issuers or HMOs with respect to such Group Health Plans, but only with respect to Protected Health Information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any such Group Health Plans.

[45 CFR 160.103.]

Password means confidential authentication information composed of a string of characters. [45 CFR 164.304.]

Patient [California] means any natural person, whether or not still living, who received health care services from a provider of health care and to whom medical information pertains. [CMIA, California Civil Code 56.05 (h).]

Payment means:

1. The activities undertaken by:

    A. A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

    B. A health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

    A. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

    B. Risk adjusting amounts due based on enrollee health status and demographic characteristics;

    C. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

    D. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

    E. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and

    F. Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:

        i. Name and address;

        ii. Date of birth;

        iii. Social security number;

iv. Payment history;

v. Account number; and

vi. Name and address of the health care provider and/or health plan.

[45 CFR 164.501.]

Person means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private. [45 CFR 160.103.]

Personal Information [California] means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or California Identification Card number; (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (4) Medical information; (5) Health insurance information; however, personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records. [California Civil Code §1798.29]

Physical Safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. [45 CFR 164.304.]

Privacy Rule refers to that portion of the HIPAA regulations (appearing as Subpart E of Part 164 of Title 45 of CFR §§164.500 to 164.534 inclusive) that took effect on April 14, 2003, and that established the requirements for covered entities concerning the use and disclosure of Protected Health Information.

Protected Health Information (PHI) means individually identifiable health information that is transmitted by or maintained in electronic media; or transmitted or maintained in any other form or medium; except for individually identifiable health information in:

- Education records covered by the Family Educational Rights and Privacy Act (FERPA)
- Student health records made or maintained by a physician or other health care professional which are used only in connection with the provision of treatment to the student and which are not available to anyone other than persons providing such treatment or other health care professional who has been asked to review such records by the student; and
- Employment records held by the University in its role as employer. [45 CFR 160.103]

Provider of Health Care (Health Care Provider) [California] means any person licensed or certified pursuant to Division 2 (Healing Arts, commencing with § 500) of the California Business and Professions Code; the Osteopathic Initiative Act; the Chiropractic Initiative Act; Division 2.5 (Emergency Medical Services, commencing with § 1797) of the Health and Safety Code; or any clinic, health dispensary, or health facility licensed pursuant to Division 2 (Licensing Provisions, commencing with § 1200) of the Health and Safety Code. [California Civil Code §56.05 (j).]

Reportable Incident means, for the purpose of this policy, any Breach, Unauthorized Access, or other Security Incident involving individually identifiable health information under any state or federal law or regulation applicable to the University, any Health Care Component of the University as designated pursuant to HIPAA regulations or any other University unit or component that maintains such information.

Required**,** as applied to an Implementation Specification (see definition above), indicates that the Implementation Specification must be implemented by the covered entity or a health care component of a hybrid entity. All Implementation Specifications are either Required or Addressable (see "Addressable" above). [45 CFR 164.306(d)(2).]

Required By Law means a mandate contained in law that compels an entity to make a use or disclosure of Protected Health Information and that is enforceable in a court of law, including, but not limited to: court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits. [45 CFR 164.103]

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System. [45 CFR 164.304.]

Security or ***Security Measures*** encompass all of the administrative, physical, and technical safeguards in an Information System. [45 CFR 164.304.]

Security Rule is a reference to that portion of the HIPAA regulations appearing as Subpart C, Part 164, 45 CFR §§164.300 to 164.318 inclusive, that took effect on April 21, 2005, and that established administrative, physical, and technical security safeguards required for the use of Protected Health Information in electronic form. For each type of safeguard, the Rule identifies various security standards, and for each standard, it sets out required and/or addressable implementation specifications.

Single Health Care Component (SHCC) means those health care components of the various campuses and locations of the University that carry out health care treatment, payment, and operations, and related health care administrative and technical support functions, considered a single covered component as defined in the HIPAA regulations, distinct from the other components, organizational units or functions of the University.

Single Health Plan Component (SHPC) means those health plan components of the various campuses and locations of the University, that carry out health plan functions, and related administrative and technical support functions, considered a single covered component as defined in the HIPAA regulations, distinct from the other components, organizational units or functions of the University.

Standard is a rule, condition, or requirement (1) Describing the following information for products, systems, services or practices: (i) Classification of components. (ii) Specification of

materials, performance, or operations; or (iii) Delineation of procedures; or (2) Referring to the privacy of individually identifiable health information. [45 CFR 160.103.]

Technical Safeguards means the technology and the policy and procedures for its use that protect electronic Protected Health Information and control access to it. [45 CFR 164.304.]

Transaction means the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmissions:

- Health care claims or equivalent encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claim status.
- Enrollment and disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.
- First report of injury.
- Health claims attachments.
- Other transactions that the DHHS Secretary may prescribe by regulation.

[45 CFR 160.103.]

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. [45 CFR 164.501.]

Unauthorized [California] means the inappropriate access, review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the California CMIA or by any other statute or regulation governing the lawful access, use, or disclosure of medical information. [California Health & Safety Code § 1280.15 (i), as amended by Senate Bill No. 541, effective January 1, 2009]

Unsecured PHI means PHI [or other individually identifiable health information] that is not secured through:

(a) valid encryption technology processes for:

> (i) data at rest that are consistent with NIST Special Publication 800-111 (Guide to Storage Encryption Technologies for End User Devices) and

(ii) data in motion that comply with the requirements of Federal Information Processing Standards (FIPS) 140-2, and

(b) the destruction of the media on which the PHI is stored or recorded in one of the following ways:

(i) the paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed; and

(ii) the electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88 (Guidelines for Media Sanitization) such that the PHI cannot be retrieved. [DHHS Guidance Specifying the Technologies and Methodologies that Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, published April 17, 2009]

User means a person or entity with authorized access. [45 CFR 164.304.]

Workforce means employees, including temporary agency or contract employees, health care professionals, including medical students and interns, volunteers, trainees, and other persons whose conduct, in the performance of work for the University's SHCC or SHPC, or a component of the SHCC or SHPC, is under the direct control of the University, whether or not they are paid by the University. [45 CFR 160.103.]

Workstation means an electronic computing device, for example, a laptop or desk computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. [45 CFR 164.304.]

Acronyms

ACE – Affiliated Covered Entity

ARRA – the American Recovery and Reinvestment Act of 2009

BA – Business Associate

BAA – Business Associate Agreement

BAC – Business Associate Contract (same as Business Associate Agreement)

CFR – Code of Federal Regulations

CIO – Chief Information Officer

CMIA –Confidentiality of Medical Information Act (California law)

CE – Covered Entity

DHHS – the U.S. Department of Health & Human Services

EPHI – Electronic Protected Health Information

HHS – see DHHS

HIPAA – the Administrative Simplification provisions of the Health Insurance Portability & Accountability Act

HITECH – the Health Information Technology for Economic and Clinical Health Act that appears as Title XIII of Division A of ARRA

ID – Identification

IIHI – Individually-Identifiable Health Information

IRB – Institutional Review Board

IS – Information System

IT – Information Technology

LAN – Local Area Network

LDS – Limited Data Set

MOU – Memorandum of Understanding

OHCA – Organized Health Care Arrangement

PHI – Protected Health Information

SHCC – Single Health Care Component

SHPC – Single Health Plan Component

UC – the University of California

Related Documents

45 CFR § 46, Subpart A

45 CFR §§ 160, 162, 164

HITECH Act § 13400 (42 USC § 17921)

California Civil Code Section 56, *et seq*.

California Civil Code §§ 1798.29, 1798.82

California Health & Safety Code § 1280.15

Federal Information Processing Standards (FIPS) 140-2

NIST Special Publication 800-88

NIST Special Publication 800-111

Revision History

HIPAA Privacy Rule: University of California Systemwide Standards and Implementation Policies (System Standards), April 2003.